(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. Juli 2001 (26.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/54057 A1

(51) Internationale Patentklassifikation[7]: G06K 19/073, G07F 7/10

(21) Internationales Aktenzeichen: PCT/EP00/13136

(22) Internationales Anmeldedatum:
22. Dezember 2000 (22.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
00 100 995.0 19. Januar 2000 (19.01.2000) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Strasse 53, 81669 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **HORVAT, Helmut** [AT/AT]; Petri Au 8a, A-8042 Graz (AT). **WALLSTAB, Stefan** [DE/DE]; Gustav-Heinemann-Ring 5, 81739 München (DE).

(74) Anwalt: **EPPING HERMANN & FISCHER**; Postfach 12 10 26, 80034 München (DE).

(81) Bestimmungsstaaten *(national)*: BR, CN, IN, JP, KR, MX, RU, UA, US.

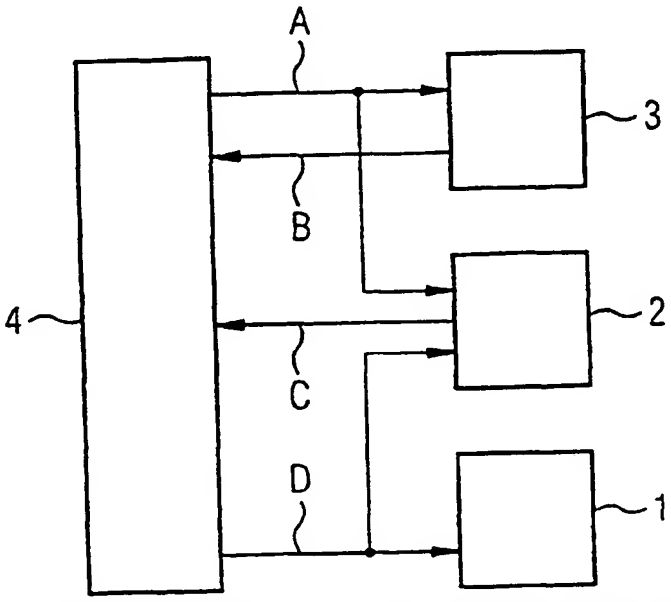
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: INTEGRATED PROTECTIVE CIRCUIT

(54) Bezeichnung: INTEGRIERTE SICHERHEITSSCHALTUNG



(57) **Abstract:** An integrated protective circuit, such as a microcontroller for chip cards, contains a function unit (1) which executes the protective function. A control device determines the number of times that the protective function is executed over time. In the event that a threshold value is exceeded, any further execution of the protective function is blocked. An analogue clock (3), comprising a charge storage device and also measuring the expiring time when the supply voltage (VDD, VSS) is switched off, is preferably provided to this end. A usage meter (2) is updated each time that the protective function is invoked. The inventive protective circuit provides increased protection against statistical attacks, is simple to produce and is compatible with existing systems.

(57) **Zusammenfassung:** Eine integrierte Sicherheitsschaltung, beispielsweise ein Microcontroller für Chipkarten, enthält eine Funktionseinheit (1), die eine Sicherheitsfunktion ausführt. Eine Steuerungseinrichtung ermittelt die Anzahl der Ausführungen der Sicherheitsfunktion pro Zeit. Bei Überschreiten eines Schwellwerts wird die weitere Ausführung der Sicherheitsfunktion blockiert. Hierzu ist vorzugsweise eine einen Ladungsspeicher umfassende analoge Uhr (3) vorgesehen, die auch bei abgeschalteter Versorgungsspannung (VDD, VSS) die verstreichende Zeit misst. Ein Benutzungszähler (2) wird bei jedem Aufruf der Sicherheitsfunktion aktualisiert. Die Sicherheitsschaltung bietet erhöhten Schutz gegen statistische Angriffe. Der Aufwand für die Realisierung ist vertretbar gering. Die Sicherheitsschaltung ist mit bisherigen Systemen kompatibel.

WO 01/54057 A1

Beschreibung

Integrierte Sicherheitsschaltung

Die Erfindung betrifft eine integrierte Sicherheitsschaltung mit einer Funktionseinheit zur Ausführung einer Sicherheitsfunktion.

Integrierte Sicherheitsschaltungen werden beispielsweise in Chipkarten verwendet. Die Schaltung ist monolithisch in einem Microcontroller integriert und berechnet beispielsweise die Ver- und Entschlüsselung des Datenverkehrs zwischen dem Microcontroller und einem Lesegerät. Die sicherheitssensitiven Funktionen des Microcontrollers der Chipkarte sind unberechtigten, betrügerischen Angriffen mit dem Ziel, die Daten zu entschlüsseln, ausgesetzt. Eine bekannte Angriffsmethode besteht darin, interessierende sicherheitssensitive Funktionen immer wieder mit nach geeigneten Kriterien sortierten Daten auf den Microcontroller anzuwenden. Auf die dadurch erhaltenen Meßwerte werden spezielle statistische Verfahren und Korrelationsmaßnahmen angewandt, um Informationen zu erhalten, die ermöglichen, den Datenverkehr von und zur Chipkarte zu entschlüsseln. Zur Ermittlung eines kryptographischen Schlüssels kann es erforderlich sein, die Chipkarte etwa 10.000 mal zu aktivieren und jedesmal festzustellen, ob der Microcontroller den Zugriff als berechtigt akzeptiert oder unberechtigt ablehnt. Bekannte Microcontroller lassen in der Praxis solche Angriffsversuche in beliebiger Vielzahl zu. Nach einer Versuchszeit von mehreren Stunden oder Tagen könnte dann der kryptographische Schlüssel rekonstruiert werden.

Bisherige Methoden, um statistische Angriffe abzuwehren, zielen beispielsweise darauf ab, die Meßwerte durch Überlagerung von Störsignalen oder zeitlicher Verschiebung des Nutzsignals so zu verfälschen, daß statistische Analysen erschwert wer-

den. Bei wirksamer Auslegung verlangsamt sich die Verarbeitungsgeschwindigkeit in der Nutzanwendung. Bei geringerem Aufwand an Signalverfälschung könnte der Schutz aber nicht ausreichen.

Eine andere bekannte Möglichkeit besteht darin, den verwendeten Schlüssel nach einer bestimmten Anzahl von Benutzungen zu aktualisieren, beispielsweise durch Fortschreiben des Schlüssels mittels einer Einwegfunktion, beispielsweise einer Hash-Funktion oder mittels des N-Count-Verfahrens. Ein Nachteil dieser Maßnahmen besteht darin, daß nicht nur der Microcontroller der Chipkarte entsprechend ausgebildet sein muß, sondern das gesamte Sicherheitssystem einschließlich aller bisher bereits ausgegebenen Chipkarten und der Lesegeräte.

Die Aufgabe der Erfindung besteht darin, eine integrierte Sicherheitsschaltung anzugeben, die eine höhere Sicherheit gegenüber unberechtigten Angriffen hat.

Gemäß der Erfindung wird diese Aufgabe durch eine integrierte Sicherheitsschaltung gelöst, die umfaßt: eine Funktionseinheit, die ausgestaltet ist, eine Sicherheitsfunktion auszuführen, eine Steuerungseinrichtung, die ausgestaltet ist, die Anzahl der Ausführungen der Sicherheitsfunktion durch die Funktionseinheit pro Zeit zu ermitteln und in Abhängigkeit davon die weitere Ausführung der Sicherheitsfunktion durch die Funktionseinheit freizugeben oder zu blockieren.

Bei der Sicherheitsschaltung gemäß der Erfindung wird die Anzahl der Benutzungen pro Zeiteinheit als Kriterium für ein Blockieren der Sicherheitsfunktion verwendet. Bei entsprechender Auslegung der Parameter kann dadurch erreicht werden, daß die Zeit zur Ermittlung hinreichend vieler Meßdaten für einen Angreifer unattraktiv lang wird. Die Rechenleistung des Microcontrollers wird durch die zusätzlichen Maßnahmen nicht

nennenswert weiter belastet. Die erforderliche Verarbeitungsgeschwindigkeit wird daher nicht erhöht. Zwar sind zusätzliche Schaltungsmaßnahmen erforderlich, der Schaltungsaufwand ist jedoch gering. Die Schnittstelle zum Gesamtsystem verändert sich nicht, so daß die Sicherheitsschaltung gemäß der Erfindung kompatibel mit entsprechenden bisherigen Schaltungen ist.

In Ausgestaltung der die Anzahl der Ausführungen der Sicherheitsfunktion pro Zeit ermittelnden Steuerungseinrichtung sind zwei Zähleinrichtungen vorgesehen. Einer der Zähler, der Benutzungszähler, wird bei jedem Aufruf der Sicherheitsfunktion inkrementiert (Aufwärtszähler) oder alternativ dekrementiert (Abwärtszähler). Eine Zeitmeßeinrichtung mißt die verstreichende absolute Zeit. Beim Initialisieren der Schaltung wird die Zeitmeßeinrichtung aufgeladen und die Zähleinrichtung auf einen vorbestimmten Wert gesetzt. Wenn die Zähleinrichtung einen Schwellwert erreicht, ohne daß die Zeitmeßeinrichtung abgelaufen ist, wird die Ausführung der Sicherheitsfunktion blockiert. Insgesamt ergibt sich, daß die Anzahl der Ausführungen der Sicherheitsfunktion pro Zeit gemessen wird und beim Überschreiten einer vorgegebenen Anzahl die Ausführung der Sicherheitsfunktion blockiert wird.

Zweckmäßigerweise wird die Zeitmeßeinrichtung so ausgeführt, daß sie auch bei abgeschalteter Versorgungsspannung arbeitet. Wenn die Zeitmeßeinrichtung abgelaufen ist, entweder unter Versorgungsspannung stehend oder ohne Versorgungsspannung, wird ein Ablaufsignal ausgegeben, so daß die Zeitmeßeinrichtung sowie die Benutzungszähleinrichtung wieder aufgeladen werden können. Nach einem Rücksetzen der Benutzungszähleinrichtung wird die Sperre für die Sicherheitsfunktion aufgehoben. Alternativ ist es auch möglich, daß beim Überschreiten des Schwellwerts durch den Benutzungszähler die Sicherheits-

schaltung permanent gesperrt und dadurch unbrauchbar gemacht wird.

Dadurch daß die Zeitmeßeinrichtung auch während abgeschalteter Versorgungsspannung läuft, ist es nicht möglich, daß durch schnelles Ab- und Anschalten der Versorgungsspannung ein schnellerer Ablauf der Uhr und dadurch eine höhere Anzahl von Meßwerten bei einem Angriff erreicht wird. Die Zeitmeßeinrichtung kann analog oder digital ausgeführt werden. Eine analoge Zeitmeßeinrichtung verwendet einen Ladungsspeicher, welcher nach dem Aufladen entladen wird, wobei der Entladevorgang auch nach Abschalten der Versorgungsspannung weiter läuft. Eine digitale Zeitmeßeinrichtung kann als Vorwärts- oder Rückwärtszähler realisiert sein, wobei ein Energiespeicher, beispielsweise eine Batterie, die Stromversorgung speziell für den Zähler weiter aufrecht erhält. Die übrigen Schaltungen des Microcontrollers werden nicht versorgt.

Die analoge Ausführungsvariante der Zeitmeßeinrichtung umfaßt einen Kondensator, der bei der Initialisierung aufgeladen wird und anschließend nur noch über Leckstromverluste entladen wird. Zur Realisierung des Kondensators ist es zweckmäßig, einen der Pole des Kondensators - mit Ausnahme der Anschlußfläche - von Dielektrikum zu umgeben. Das Dielektrikum kann Siliziumdioxid oder Siliziumnitrid sein. Dieser Pol ist dann ausreichend gut isoliert, so daß von der Plattenfläche selbst kaum Leckströme abfließen. Der Kondensator wird von einem Schalttransistor in MOS-Halbleitertechnologie angesteuert. Bei leitendem Schalttransistor wird der Kondensator aufgeladen; bei abgeschaltetem Schaltransistor entlädt sich der Kondensator nur über Leckströme, die über dasjenige Elektrodengebiet abfließen, welches mit dem betreffenden Kondensatorpol verbunden ist. Durch Steuerung des Substratanschlusses des Schalttransistors kann dessen Verhalten im leitenden und gesperrten Zustand weiterhin verbessert werden. Die am Kon-

densator anliegende Spannung wird über einen Komperator abgefragt, um den entladenen Zustand festzustellen und das Ablaufsignal zu aktivieren.

Die Entladekennlinie des Kondensators ist temperaturabhängig. Bei erhöhter Temperatur wird der Kondensator stärker entladen als bei niedriger Temperatur. Jedoch kann die Sicherheitsfunktion nur bei üblichen Betriebstemperaturen ausgeführt werden, um dementsprechende Meßwerte für einen statistischen Angriff zu erhalten. Die für das Erwärmen und Abkühlen erforderliche Zeitdauer verhindert, daß ausreichend viele Meßwerte in vernünftiger Zeit erzeugt werden. Eine Zeitbasis, die auf der Entladung von sog. Traps an Nitrit-Schichten über Fowler-Nordheim-Tunneling basieren, ist temperaturunabhängig und als Speichermedium alternativ zu einem Kondensator geeignet.

Für die Benutzungszähleinrichtung gibt es verschiedene Realisierungsmöglichkeiten. Der Benutzungszähler kann als reiner Softwarezähler ausgeführt werden, bei dem der Zählwert nur durch die zentrale Verarbeitungseinheit (CPU) des Microcontrollers inkrementiert bzw. dekrementiert und ausgewertet wird. Nach jeder Aktualisierung wird der Zählwert zweckmäßigerweise in den auf dem Microcontrollerchip ohnehin enthaltenen nichtflüchtigen Speicher (NVM) zurückgeschrieben, so daß er auch nach einem Spannungsausfall erhalten bleibt. Es sind auch Mischformen aus Hardware- und Softwarezähler möglich, insbesondere wenn die Benutzung eines Coprozessors überwacht werden soll. Die CPU liest den aktuellen Wert des Benutzungszählers aus dem NVM aus und schreibt ihn als Startwert in einen Hardwarezähler. Außerdem wird der Schwellwert in den Hardwarezähler geladen, bei dessen Erreichen das Blockierungssignal erzeugt wird. Der Endwert kann aber auch in einem ROM-Speicher stehen. Wird der Schwellwert erreicht, bleibt der Hardwarezähler stehen und sperrt den Coprozessor. Der Schwellwert kann außerdem vorsorglich ins NVM geschrieben

werden, um die Information auch beim Trennen der Versorgungsspannung zu erhalten. Nach Abschluß der Operation des Coprozessors wird der tatsächliche Zählerstand in das NVM geschrieben. Alternativ könnte der Hardwarezähler auch direkt auf das NVM zugreifen.

Die Benutzungszähleinrichtung kann auch als Analogschaltung ausgeführt werden. Der Zählerstand wird dann durch die Menge der Ladung in einem Ladungsspeicher repräsentiert. Dadurch wird Unabhängigkeit von einem Betriebstakt erreicht. Wenn sowohl der Betriebszähler als auch die Uhr als Analogschaltungen ausgeführt sind, besteht die die Anzahl der Benutzungen pro Zeiteinheit repräsentierende Information im Verhältnis der Spannungsverhältnisse der beiden Ladungsspeicher. Die Ladungsspeicher von Uhr und Benutzungszähler werden zunächst auf unterschiedliche Spannungen vorgeladen. Bei jedem Aufruf der Sicherheitsfunktion wird ein kurzzeitiger, unvollständiger Ladungsausgleich ausgeführt. Bei Erreichen eines bestimmten Spannungsverhältnisses, beispielsweise beide Spannungen sind gleich, wird festgestellt, daß die höchst zulässige Anzahl von Benutzungen der Sicherheitsfunktion pro Zeit erreicht ist. Ein weiterer Aufruf der Sicherheitsfunktion wird dann blockiert.

Nachfolgend wird die Erfindung anhand der in der Zeichnung dargestellten Figuren näher erläutert. Es zeigen

Figur 1 ein Prinzipschaltbild einer integrierten Sicherheitsschaltung gemäß der Erfindung,

Figur 2 ein Blockschaltbild mit erfindungsrelevanten Elementen eines Microcontrollers und

Figur 3 eine analog arbeitende schaltungstechnische Realisierung einer Zeitmeßeinrichtung, die für die Sicherheitsschaltung der Erfindung geeignet ist.

Die Schaltung in Figur 1 zeigt eine Zeitmeßeinrichtung oder Uhr 3, einen Benutzungszähler 2 sowie eine Funktionseinrichtung 1, die eine Sicherheitsfunktion ausführt. Eine Steuerungseinrichtung 4 dient zur Ablaufsteuerung. Die Schaltung ist in einem Microcontroller enthalten, der auf einer Chipkarte angeordnet ist. Die Funktionseinheit 1 führt eine Ver- und Entschlüsselung des Datenverkehrs zwischen Chipkarte und Lesegerät aus.

Um statistische Angriffe zur etwaigen Ermittlung der Funktionscharakteristik oder gar des Schlüssels der Einrichtung 1 zu verhindern, ist vorgesehen, die Anzahl der Benutzungen der Funktionseinheit 1 pro Zeiteinheit zu begrenzen. Hierzu wird die Uhr 3 durch ein Steuersignal A aus der Steuerungseinrichtung 4 aufgeladen, um von nun an abzulaufen. Ein Ablaufsignal B, welches von der Uhr 3 an die Steuerungseinrichtung 4 zurückgegeben wird, zeigt an, daß die von der Uhr 3 gemessene absolute Zeit verstrichen ist. Die Uhr 3 kann als Digitalzähler oder Analogzähleinrichtung ausgeführt sein. Ein analoges Ausführungsbeispiel ist in Figur 3 gezeigt.

Der Benutzungszähler 2 ist ein Digitalzähler, welcher ebenfalls mit dem Aufladen der Uhr 3 initialisiert, d.h. auf einen vorbestimmten Wert gesetzt wird. Mit jedem Aufruf der Funktionseinheit 1 durch das Signal D wird der Benutzungszähler 2 inkrementiert. Wenn der Zähler 2 einen vorbestimmten Maximalwert erreicht, wird das Signal C aktiviert. Die Steuerungseinrichtung 4 schließt bei noch nicht abgelaufener Uhr 3 und Erreichen des Maximalwerts des Zählers 2 daraus, daß eine vorbestimmte Anzahl von Aufrufen der Sicherheitsfunktion in der Einheit 1 pro durch die Uhr 3 festgelegter Zeitdauer erreicht worden ist. Die Steuereinheit 4 blockiert daraufhin jeden weiteren Aufruf der Sicherheitsfunktion in der Funktionseinheit 1. Im beschriebenen Beispiel ist der Benutzungszähler 2 ein Aufwärtszähler. Er kann alternativ als Abwärts-

zähler ausgeführt werden, der bei Initialisierung auf einen Startwert gesetzt wird und dann bis zu einem Endwert, beispielsweise den Zählerstand Null, dekrementiert wird.

Die Uhr 3 ist derart ausgeführt, daß sie auch bei abgeschalteter Versorgungsspannung weiterläuft und die verstreichende Zeit absolut mißt. Auch der Benutzungszähler 2 speichert den momentanen Benutzungszählwert nach Abschalten der Versorgungsspannung. Hierzu wird der momentane Zählerstand des Zählers 2 in einem nichtflüchtigen Speicher, der ohnehin auf dem Microcontroller vorhanden ist, zwischengespeichert. Alternativ ist eine Batteriepufferung möglich.

Die Bewertung, ob die Uhr abgelaufen ist, kann einstellbar ausgeführt werden, um sowohl hinsichtlich des Parameters Benutzung als auch hinsichtlich des Parameters Zeitdauer Flexibilität zu erhalten. Für manche Zwecke kann die Gewährung von fünf Benutzungen pro fünf Minuten ausreichend sein, für andere Zwecke die Messung über einen größeren Zeitraum sinnvoll sein, z.B. 60 Benutzungen pro Stunde. Diese 60 Benutzungen können dann aber durchaus in den ersten fünf Minuten der Stunde stattfinden.

Der Microcontroller 10 in Figur 2 weist eine zentrale Verarbeitungseinheit CPU 11 auf. Diese steuert die Betriebsabläufe und führt Berechnungen aus. In einem nichtflüchtigen Speicher NVM 12 können Daten auch nach Abschalten der Versorgungsspannung dauerhaft gespeichert werden. CPU 11 und NVM 12 kommunizieren über einen chipinternen Bus 13. Die Uhr 3 ist als separater Schaltungsblock vorgesehen. Die die Uhr 3 steuernden Signale A, B werden über den Bus 13 bereitgestellt. Der Benutzungszähler 2 ist als weiterer separater Schaltungsblock auf dem Chip des Microcontrollers 10 angeordnet. Er wird mit den Signalen A und D über den Bus 13 versorgt. Die Funktionseinheit 1 wird von der CPU 11 und entsprechender Software-

steuerung realisiert. Wenn der Zähler 2 den vorgegebenen Endwert erreicht, wird dieser Zustand der CPU 11 als Steuerungssignal C angezeigt. Der Benutzungszähler 2 erhält den Start- und den Endwert aus dem NVM 12. Nach jedem Aktualisieren des Zählerstands des Zählers 2 wird dieser in das NVM 12 zurückgeschrieben, um ihn auch bei einem Wiedereinschalten der Versorgungsspannung nach einem Abbruch der Versorgungsspannung zur Verfügung zustellen, wenn die Uhr 3 noch nicht abgelaufen ist.

Die Uhr 3 wird zweckmäßigerweise als Analogzähler ausgeführt. Ein Ausführungsbeispiel ist in Figur 3 dargestellt. Die Uhr umfaßt einen Ladungsspeicher 31, dessen Ladungszustand die abgelaufene Zeit repräsentiert. Der Ladungsspeicher 31 ist ein Kondensator. Ein Schalttransistor 32 bildet mit dem Kondensator 31 eine Reihenschaltung, die zwischen Versorgungsspannungsanschlüsse für die Versorgungspotentiale VDD und VSS geschaltet sind. Der Schalttransistor 32 ist in MOS-Schaltungstechnik als N-Kanal-Transistor ausgeführt und dient zum Laden und Entladen des Kondensators 31. Zum Aufladen der Uhr, d.h. zum Laden des Kondensators 31 wird das Signal A am Gateanschluß des Schalttransistors 32 aktiviert, so daß der N-Kanal-MOS-Transistor 32 leitend wird. Der Kondensator 31 wird aus dem Versorgungspotential VDD aufgeladen. Ein zwischen Gateanschluß des Transistors 32 und Anschluß für Masse VSS geschalteter Widerstand 33 dient zum sicheren Abschalten des Transistors 32, wenn das Signal A deaktiviert ist.

Um Leckstromverluste am Kondensator 31 möglichst gering zu halten, wird einer seiner Pole, beispielsweise der mit dem Transistor 32 verbundene Pol, vollständig von Siliziumoxid oder Nitrid umgeben, abgesehen von der Verbindungsleitung zwischen Kondensatorplatte und Transistor 32. Siliziumoxid und Nitrid bilden außerdem das Dielektrikum des Kondensators 31. Realisiert werden kann dies dadurch, daß eine Me-

tall1-Schicht mit dem Gate-Polisilizium zu einem Pol zusammengefaßt wird. Der erste Pol ist mit dem Transistor 32 verbunden. Eine Metall2-Schicht, Substrat und Poly2-Schicht bilden den zweiten, an Masse VSS angeschlossenen Pol. Metall1- und Metall2-Schichten sind dabei zwei übereinanderliegende Metallisierungen.

Bei abgeschaltetem Schalttransistor 32 ist die Ladung im Kondensator 31 gespeichert und entlädt sich nur über sich im Halbleiterkörper einstellende Leckstrompfade. Die Ladung bleibt auch nach Abschalten der Versorgungsspannung VDD, VSS im Kondensator 31 erhalten. Durch die Isolierung des mit dem Schalttransistor verbundenen Pols des Kondensators 31 sind Leckstromverluste von diesem Pol direkt ins Substrat nicht vorhanden. Die Entladung des Kondensators 31 kann daher nur über die Dotierungsstruktur des kondensatorseitigen Anschlusses 32a des Schalttransistors 32 erfolgen. Der N-Kanal-MOS-Transistor 32 ist in einer P-Wanne ausgeführt. Es stellen sich dort geringe Leckströme ein, die sich im Pfad zwischen dem den Anschluß 32a des Transistors 32 bildenden Dotierungsgebiet, der Wanne und dem Substrat ausbilden. Die Entladungsstrecke ist ausreichend hochohmig, um eine entsprechend lange Zeitdauer durch die Uhr messen zu können. Andererseits aber wird die Entladung in angemessener Zeit beendet. Die Entladungsrate liegt in der Größenordnung von 1 $fA/\mu m^2$ bei Raumtemperatur. Die Entladungsrate kann durch entsprechende geometrische Anpassung der Dotierungsstrukturen skaliert werden. Zweckmäßigerweise wird das Dotierungsgebiet des Anschlusses 32a von der Substratoberfläche aus rund ausgeführt, um eine minimale Kontaktfläche zur P-Wanne zu erhalten. Bei anliegender Versorgungsspannung VDD, VSS wirkt der Anschluss 32a als Source-Anschluß des Transistors 32; bei abgeschalteter Versorgungsspannung kehren sich die Spannungsverhältnisse um, so daß der Anschluß 32a als Gate-Elektrode wirkt. Die am Kondensator 31 anliegende Spannung wird von ei-

nem Komparator 36 abgefragt. Der Komparator 36 ist bei anliegender Versorgungsspannung VDD, VSS aktiv. Er vergleicht die am Kondensator 31 anliegende Spannung mit einer Referenzspannung VREF. Er erzeugt daraus das Abschaltsignal B, wenn die Kondensatorspannung 31 unter die Referenzspannung VREF abgesunken ist und damit anzeigt, daß die zu messende Zeitdauer abgelaufen ist.

Der Substratanschluß 32b des Schalttransistors 32 ist über einen P-Kanal-MOS-Transistor 35 mit Masse VSS verbindbar. Der P-Kanal-MOS-Transistor 34 wird durch ein Signal F so gesteuert, daß er nach dem Abschalten des Schalttransistors 32 leitend gesteuert wird, so daß der Substratanschluß 32b des Schalttransistors 32 auf Masse VSS gelegt wird. Dadurch wird bewirkt, daß etwaige Subthreshold-Ströme durch den Kanal des Transistors 32 weiter verringert werden. Wenn demgegenüber der Schalttransistor 32 leitend geschaltet ist, um den Kondensator 31 aufzuladen, wird der Transistor 34 gesperrt, so daß über eine Kapazität 35 der Substratanschluß 32b des Schalttransistors 32 an das positive Versorgungspotential VDD angehoben wird, um den leitenden Kanal des Schalttransistors 32 noch weiter aufzusteuern.

Alternativ zu dem in Figur 3 dargestellten geschalteten Substratanschluß 32b des Schalttransistors 32 kann das Gate des Transistors 32 über eine geschaltete Kapazität negativ vorgespannt werden, d.h. das Gate wird auf ein Potential unterhalb von Masse VSS gelegt. Der Transistor 32 wird dabei noch sicherer gesperrt, um Subtreshhold-Ströme durch seinen Kanal zu vermeiden.

Patentansprüche

1. Integrierte Sicherheitsschaltung, die umfaßt:
- eine Funktionseinheit (1), die ausgestaltet ist, eine Sicherheitsfunktion auszuführen,
- eine Steuerungseinrichtung (2, 3, 4), die ausgestaltet ist, die Anzahl der Ausführungen der Sicherheitsfunktion durch die Funktionseinheit (1) pro Zeit zu ermitteln und in Abhängigkeit davon die weitere Ausführung der Sicherheitsfunktion durch die Funktionseinheit (1) freizugeben oder zu blockieren.

2. Integrierte Sicherheitsschaltung nach Anspruch 1, g e k e n n z e i c h n e t d u r c h eine Zeitmeßeinrichtung (3), die ausgestaltet ist, nach einer Initialisierung die verstreichende Zeit zu messen, eine Zähleinrichtung (2), die mit der Funktionseinheit (1) gekoppelt ist, um nach der Initialisierung jede Ausführung der Sicherheitsfunktion in der Funktionseinheit (1) zu zählen, und ein Mittel zur Vorgabe eines Schwellwerts, wobei dann, wenn die Zähleinrichtung (1) den Schwellwert überschreitet, die Ausführung der Sicherheitsfunktion durch die Funktionseinheit (1) blockiert wird, und andernfalls freigegeben wird.

3. Integrierte Sicherheitsschaltung nach Anspruch 2, d a d u r c h g e k e n n z e i c h n e t, daß Anschlüsse für eine Versorgungsspannung (VDD, VSS) vorgesehen sind, daß die Anschlüsse mit der Funktionseinheit (1) verbunden sind und die Funktionseinheit (1) ausgebildet ist, die Sicherheitsfunktion auszuführen, wenn die Versorgungsspannung (VDD, VSS) anliegt, und daß die Zeitmeßeinrichtung (3) ausgebildet ist, nach einem Anliegen der Versorgungsspannung (VDD, VSS) auch beim Nichtanliegen der Versorgungsspannung (VDD, VSS) die verstreichende Zeit zu messen.

4. Integrierte Sicherheitsschaltung nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß eine maximale Zeitdauer vorgesehen ist, während welcher die Zeitmeßeinrichtung (3) die Zeit messen kann, daß die Zeitmeßeinrichtung (3) ein Ablaufsignal (B) bereitstellt, das angibt, daß die maximale Zeit abgelaufen ist, daß die Steuerungseinrichtung (1) ausgebildet ist, die Zeitmeßeinrichtung (3) und die Zähleinrichtung bei Vorliegen des Ablaufsignals (B) erneut zu initialisieren.

5. Integrierte Sicherheitsschaltung nach Anspruch 4, dadurch gekennzeichnet, daß die Zähleinrichtung (2) ein digitaler Vorwärtszähler oder ein Rückwärtszähler ist, der bei jedem Aufruf der Sicherheitsfunktion inkrementiert bzw. dekrementiert wird, daß bei der Initialisierung der Zähler auf Null bzw. auf den vorgegebenen Schwellwert vorbesetzt wird und daß beim Überschreiten des Schwellwerts bzw. der Null ein Signal (C) erzeugt wird, um die weitere Ausführung der Sicherheitsfunktion durch die Funktionseinheit (1) freizugeben oder zu blockieren.

6. Integrierte Sicherheitsschaltung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Zeitmeßeinrichtung (3) einen Kondensator (31) umfaßt, der bei der Initialisierung aufladbar ist und anschließend nur über einen Leckstromverlust entladbar ist.

7. Integrierte Sicherheitsschaltung nach Anspruch 6, dadurch gekennzeichnet, daß der Kondensator (31) zwei Pole und ein dazwischen liegendes Dielektrikum aufweist und daß einer der Pole vom Dielektrikum umgeben ist.

8. Integrierte Sicherheitsschaltung nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß der Kondensator (31) mit einem MOS-Schalttransistor (32) eine Reihenschaltung bildet, die zwischen die Anschlüsse für eine Versorgungsspannung (VDD, VSS) geschaltet ist, daß die Gate-Elektrode des Schalttransistors (32) von einem die Initialisierung angebenden Signal (A) steuerbar ist, daß der Substratanschluß des MOS-Schalttransistors (32b) über einen weiteren MOS-Schalttransistor (34) mit einem der Versorgungspotentialanschlüsse verbindbar ist.

9. Integrierte Sicherheitsschaltung nach Anspruch 8, soweit auf Anspruch 4 rückbezogen, gekennzeichnet durch einen Komparator (36), der eingangsseitig mit dem vom Dielektrikum umgebenen Pol des Kondensators (31) und mit einem Anschluß für ein Referenzsignal (VREF) verbunden ist und der ausgangsseitig einen Anschluß für das Ablaufsignal (B) aufweist.

10. Integrierte Sicherheitsschaltung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß die Sicherheitsfunktion ein Verschlüsseln oder Entschlüsseln von Daten umfaßt.

FIG 1

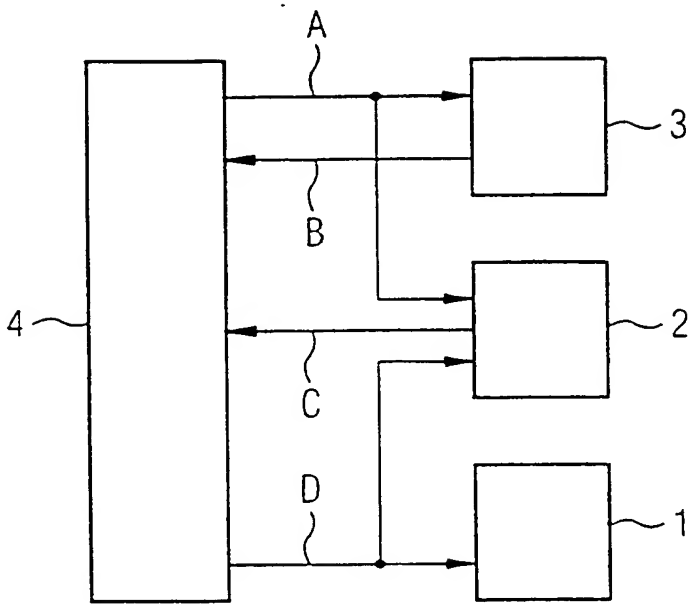


FIG 2

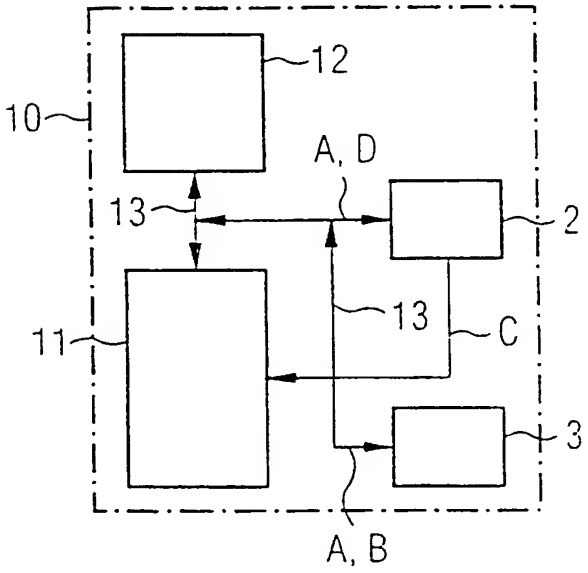
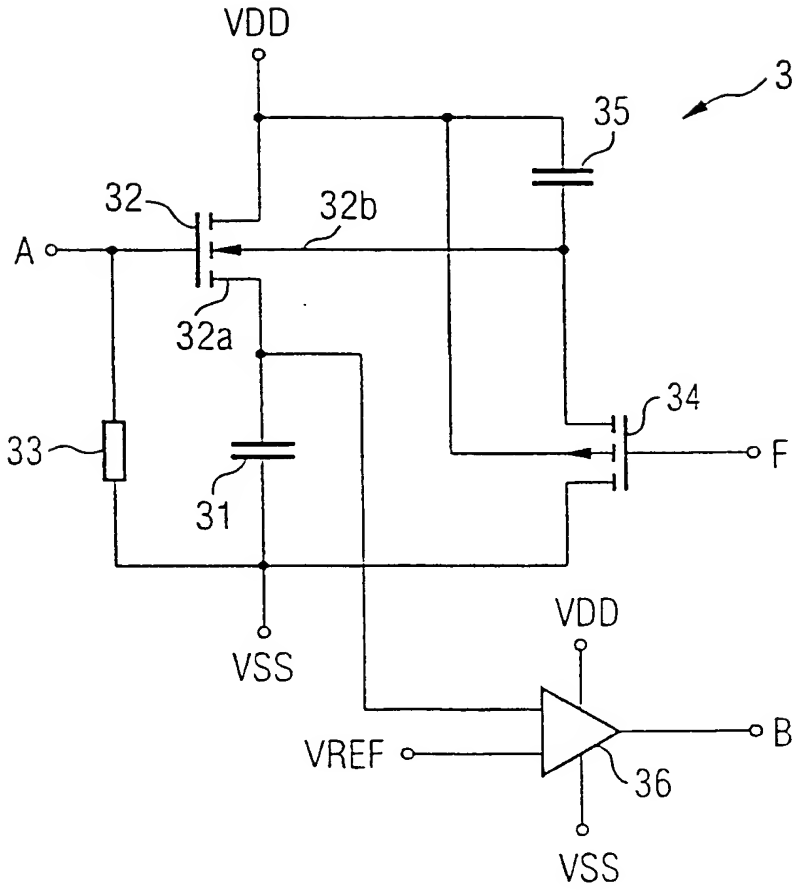


FIG 3



INTERNATIONAL SEARCH REPORT

Internatio Application No
PCT/EP 00/13136

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 56253 A (DEUTSCHE TELEKOM MOBIL) 4 November 1999 (1999-11-04) page 3 claims 3-6	1,2,4,5, 10
A	WO 88 10479 A (FANUC LTD) 29 December 1988 (1988-12-29) page 1	1,4
A	US 5 594 227 A (DEO VINAY) 14 January 1997 (1997-01-14) claim 8	1
A	FR 2 493 564 A (GAO GES AUTOMATION ORG) 7 May 1982 (1982-05-07) claims 5,6,10	6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 May 2001	30/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herskovic, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internatio Application No
PCT/EP 00/13136

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 311 360 A (INNOVATION STE INT) 10 December 1976 (1976-12-10) claim 14	9

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatic Application No
PCT/EP 00/13136

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9956253 A	04-11-1999	DE 19818830 A	28-10-1999
		EP 1075681 A	14-02-2001
WO 8810479 A	29-12-1988	JP 63316191 A	23-12-1988
US 5594227 A	14-01-1997	NONE	
FR 2493564 A	07-05-1982	DE 3041109 A	09-06-1982
		BE 890950 A	15-02-1982
		CH 656014 A	30-05-1986
		GB 2088605 A,B	09-06-1982
		IT 1145571 B	05-11-1986
		JP 1747224 C	25-03-1993
		JP 57120183 A	27-07-1982
		JP 63043791 B	01-09-1988
		JP 1727825 C	19-01-1993
		JP 2288993 A	28-11-1990
		JP 4013753 B	10-03-1992
		NL 8104842 A,B,	17-05-1982
		SE 462876 B	10-09-1990
		SE 8106354 A	01-05-1982
		SE 506491 C	22-12-1997
		SE 9001035 A	23-09-1991
		US 4484067 A	20-11-1984
FR 2311360 A	10-12-1976	DE 2621271 A	25-11-1976
		GB 1543602 A	04-04-1979
		JP 1490000 C	07-04-1989
		JP 52007649 A	20-01-1977
		JP 60001666 B	16-01-1985
		NL 7605119 A	16-11-1976
		US 4092524 A	30-05-1978

INTERNATIONALER RECHERCHENBERICHT

Internatio· ·s Aktenzeichen
PCT/EP 00/13136

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06K19/073 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06K G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
WPI Data, PAJ, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 99 56253 A (DEUTSCHE TELEKOM MOBIL) 4. November 1999 (1999-11-04) Seite 3 Ansprüche 3-6	1,2,4,5, 10
A	WO 88 10479 A (FANUC LTD) 29. Dezember 1988 (1988-12-29) Seite 1	1,4
A	US 5 594 227 A (DEO VINAY) 14. Januar 1997 (1997-01-14) Anspruch 8	1
A	FR 2 493 564 A (GAO GES AUTOMATION ORG) 7. Mai 1982 (1982-05-07) Ansprüche 5,6,10	6

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
22. Mai 2001	30/05/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Herskovic, M

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internatio· 's Aktenzeichen
PCT/EP 00/13136

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FR 2 311 360 A (INNOVATION STE INT) 10. Dezember 1976 (1976-12-10) Anspruch 14 _____	9

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/13136

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9956253	A	04-11-1999	DE	19818830 A	28-10-1999
			EP	1075681 A	14-02-2001
WO 8810479	A	29-12-1988	JP	63316191 A	23-12-1988
US 5594227	A	14-01-1997	KEINE		
FR 2493564	A	07-05-1982	DE	3041109 A	09-06-1982
			BE	890950 A	15-02-1982
			CH	656014 A	30-05-1986
			GB	2088605 A,B	09-06-1982
			IT	1145571 B	05-11-1986
			JP	1747224 C	25-03-1993
			JP	57120183 A	27-07-1982
			JP	63043791 B	01-09-1988
			JP	1727825 C	19-01-1993
			JP	2288993 A	28-11-1990
			JP	4013753 B	10-03-1992
			NL	8104842 A,B,	17-05-1982
			SE	462876 B	10-09-1990
			SE	8106354 A	01-05-1982
			SE	506491 C	22-12-1997
			SE	9001035 A	23-09-1991
			US	4484067 A	20-11-1984
FR 2311360	A	10-12-1976	DE	2621271 A	25-11-1976
			GB	1543602 A	04-04-1979
			JP	1490000 C	07-04-1989
			JP	52007649 A	20-01-1977
			JP	60001666 B	16-01-1985
			NL	7605119 A	16-11-1976
			US	4092524 A	30-05-1978